

PCI DSS DONE RIGHT OR WRONG!

Dr. Anton Chuvakin

Branden R. Williams, CISSP, CISM

Source, April 2010

AGENDA

- ✖ PCI DSS basics for security folks
- ✖ Fun PCI facts
- ✖ PCI DSS done RIGHT and WRONG
- ✖ Conclusions
- ✖ Q&A, Discussion, Brawl 😊

ABOUT BRANDEN

- ✖ Director, RSA Security Consulting
- ✖ Six plus years with PCI DSS
- ✖ Twitter: @BrandenWilliams
- ✖ Blog: blog.brandenwilliams.com
- ✖ Author: PCI Compliance



ABOUT ANTON

Email: anton@chuvakin.org

Site: <http://www.chuvakin.org>

Blog: <http://www.securitywarrior.org>

Twitter: @anton_chuvakin

- ✗ **Consultant:** <http://www.securitywarriorconsulting.com>
- ✗ **Book author:** “Security Warrior”, “PCI Compliance”, “Information Security Management Handbook”, “Know Your Enemy II”, “Hacker’s Challenge 3”, etc
- ✗ **Conference speaker:** SANS, FIRST, GFIRST, ISSA, CSI, RSA, Interop, *many, many others worldwide*
- ✗ **Standard developer:** CEE, CVSS, OVAL, etc
- ✗ **Community role:** SANS, Honeynet Project, WASC, CSI, ISSA, OSSTMM, InfraGard, ISSA, others
- ✗ **Past roles:** Researcher, Security Analyst, Strategist, Evangelist, Product Manager

WHAT IS PCI DSS OR PCI?

Payment Card Industry Data Security Standard

Payment Card =



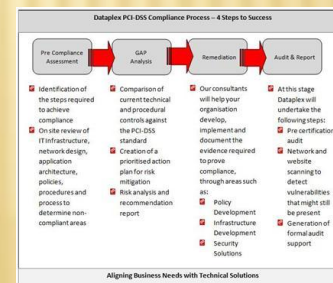
Payment Card Industry =



Data Security =



Data Security Standard =



PCI DSS = BASIC SECURITY PRACTICES

Build and Maintain a Secure Network	• Install and maintain a firewall configuration to protect data • Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	• Protect stored data • Encrypt transmission of cardholder data and sensitive information across public networks
Maintain a Vulnerability Management Program	• Use and regularly update anti-virus software • Develop and maintain secure systems and applications
Implement Strong Access Control Measures	• Restrict access to data by business need-to-know • Assign a unique ID to each person with computer access • Restrict physical access to cardholder data
Regularly Monitor and Test Networks	• Track and monitor all access to network resources and cardholder data • Regularly test security systems and processes
Maintain an Information Security Policy	• Maintain a policy that addresses information security

CEILING VS FLOOR

PCI *is* a “**floor**” of
security

This is fundamental reality of PCI DSS!

However, many prefer to
treat it as a “**ceiling**”

Result:
security breaches

PCI DSS DIFFICULTY

WRONG

Whine that “PCI DSS” is too hard – and not do it

Avoid parts that are seen as “hard” (e.g. logging)

Choose CCs that are inferior to PCI controls

RIGHT

Aim at benefiting from PCI DSS efforts (it IS possible!)

“Dual use everything” – buy for PCI, use broadly

Prioritize controls based on your risk (but aim to cover 100% of requirements)

PCI DSS EASY

WRONG

Consider that PCI is easy = [external] scan + “Y”

“QSA shop”

Think “sprint, not marathon”

RIGHT

Think “gap” – *yes, you do have it!*

Select the QSA that understands the business

Prepare to maintain it (to not be “wasn’t compliant when breached” case)

PCI DSS = SECURITY?

WRONG

Pass a PCI assessment? Think “done with security”

Only implement PCI controls; ignore everything else

Remember about PCI DSS once a quarter

RIGHT

Focus on doing security and PCI

Remember the daily tasks in PCI DSS

“Floor, not the ceiling”

TRUTH IN PCI

WRONG

Lie to QSA and/or acquirer; play scope games

Misrepresent data in SAQ

Lie to management about “we are compliant”

RIGHT

Work with good QSA to get an objective
assessment

Glance at PCI, think risk to data -> then implement

MAKING UP REQUIREMENTS

WRONG

QSA acts like black hat security hacker

QSA believes PCI is “common sense”

QSA hears trainer wrong

RIGHT

PCI DSS is a baseline tuned to cardholder data

That's why improvement to PCI DSS is imperative

Focus on printed material part of PCI DSS

COMPROMISING CONTROLS

WRONG

Treat compensating controls as shortcuts

Use ultra-liberal or ultra-conservative approach

Lose sight of the original requirement

RIGHT

Use compensating controls where needed

Use an approach that passes the “sniff test”

Meet the requirements for a valid comp control

THE FNG

WRONG

Put someone brand new on PCI DSS assessment

New Assessor (3-days of training?)

New Assessee (0-days of training!)

RIGHT

Ensure assessors are experienced

Allow new employees to shadow experienced ones

Send employees to merchant training

PCI AND SECURITY TODAY



<- This is the enemy!

This is NOT the enemy! ->



Remember:

security first, compliance as a result.

CONTINUOUS COMPLIANCE VS VALIDATION

Q: What to do after your QSA leaves?

A: PCI DSS compliance does NOT end when a QSA leaves or SAQ is submitted.

- ✗ Use what you built for PCI to reduce risk
- ✗ “Own” PCI DSS; make it the **basis** for your policies
- ✗ Think **beyond credit card data** and grow your security!

Note: a good QSA will check whether you are “wired” for continuous compliance. Pick one of that sort!

BTW, see Anton’s recent paper: “How to STAY Compliant”

CONCLUSIONS AND ACTION ITEMS

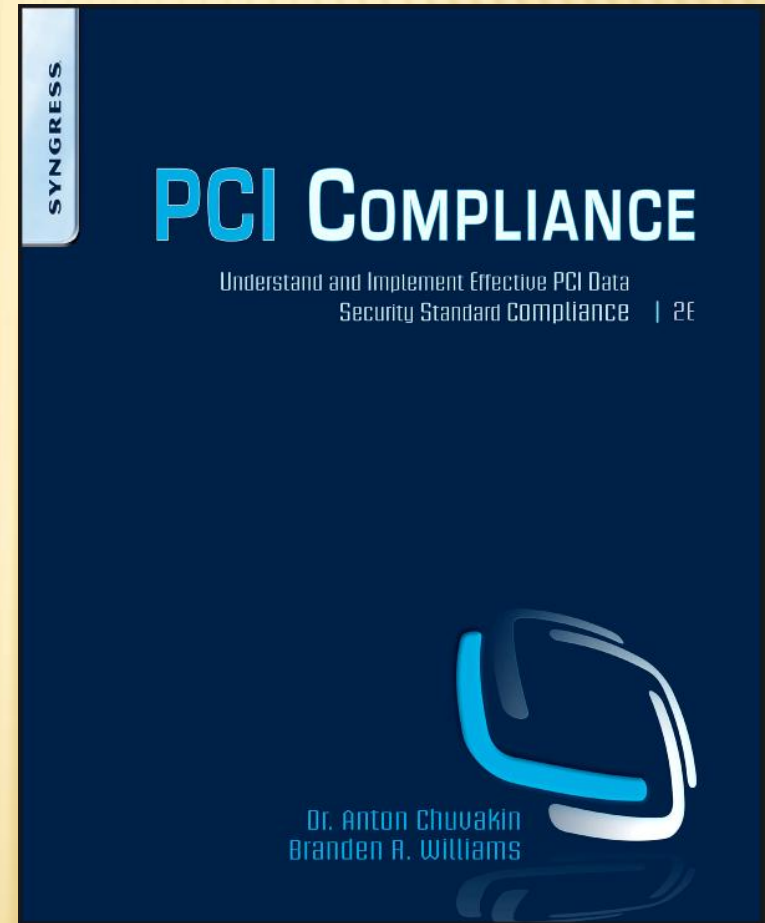
1. PCI is common sense, basic security; **stop complaining about it - start doing it!**
2. After validating that you are compliant, don't stop: **continuous compliance AND security is your goal**, not “passing an audit.”
3. Develop “**security and risk**” mindset, not “compliance and audit” mindset.

GET MORE INFO!

“PCI Compliance” by Anton Chuvakin and Branden Williams, THE PCI book for merchants, vendors – and everybody else!

Get TWO free chapters at
<http://www.pcicompliancebook.info/>

Released **December 2009!**



QUESTIONS?

Anton Chuvakin

anton@chuvakin.org

@anton_chuvakin

Branden R. Williams, CISSP, CISM

brw@brandenwilliams.com

www.brandenwilliams.com

@BrandenWilliams